AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of protecting machine readable media from unauthorized storage or copying, comprising:

sending a detector to a client process, wherein the detector comprises a sequence of different types of computer system calls;

receiving, at a server, a response to the detector from the client process;

detecting, by the server, a presence of an unauthorized software behavior on the client based upon a comparison between the response and the detector according to ~~the response and~~ a matching rule that is associated with the detector sent; and

updating a database of detectors for a previously unseen and unauthorized behavior of the process based in part on the response, such that the database of detectors evolves over time.

2. (Currently Amended) The method as in claim 1, wherein the sent detector includes at least one of a self-detector, a memory detector, and a novel detector, and wherein:

the self-detector comprises a sequence of different types of system calls detectable in a normal execution of a process;

the memory detector comprises a sequence of different types of system calls that is associated with a known unauthorized process alteration; and

the novel detector comprises a sequence of different types of system calls that has not been previously detected in an execution of the process.

3. (Original) The method as in claim 1, wherein the sent detector further comprises detecting the presence of an unauthorized substantially simultaneously executing client process.

4. (Currently Amended) The method as in claim 1, wherein the sending of the detector further comprises varying a ~~sequence~~ length of the sequence of computer system calls within the detector such that the meaning of the detector is obscured.

5. (Original) The method as in claim 1, wherein the sending of the detector further comprises encoding numerically the detector such that the meaning of the detector is obscured.

6. (Original) The method as in claim 1, wherein the matching rule includes a criterion for each field in the detector that is to be matched before a match is validated, wherein each field includes a sequence of at least one computer system calls.

7. (Original) The method as in claim 1, further including sending the detector to detect previously unseen and unauthorized behavior to another client process.

8. (Currently Amended) The method as in claim 1, further including:

exchanging sets of memory detectors between the server and another server during an update period, wherein each memory detector comprises a sequence of different types of system calls that is associated with a known unauthorized process alteration;

evaluating the received set of memory detectors against each server's self database of detectors and a set of matching rules;

discarding memory detectors in the received set of memory detectors that match another detector in each server's self database of detectors, wherein a false positive detection is minimized; and

merging each new retained memory detector from the received set of memory detectors with each server's memory database of detectors, wherein the exchange of the sets of memory detectors between each server obstructs the spread of unauthorized copying and corruption of electronic media.

9. (Currently Amended) A method for obstructing unauthorized copying and corruption of media between clients that communicate over a network of servers, comprising:

exchanging a set of memory detectors between servers during an update period, wherein each memory detector comprises a sequence of different types of system calls that is associated with a known unauthorized process alteration;

evaluating each received set of memory detectors against each server's self database and a set of matching rules;

discarding each detector in the received set of detectors that match another detector in each server's self database; and

merging a new retained detector from each received set of detectors with each server's memory database, wherein the exchanging of the set of memory detectors prevents unauthorized copying and corruption of media.

10. (Currently amended) The method as in claim 9, wherein each detector within the set of memory detectors has a life span wherein the detector is active on a client during the life span and becomes inactive when the life span is exceeded. ~~include at least one of a self detector, a memory detector, and a novel detector~~.

11. (Original) The method as in claim 9, wherein the set of detectors enable the detection of the presence of an unauthorized substantially simultaneously executing client process.

12. (Original) The method as in claim 9, wherein the exchanging the set of memory detectors further includes varying a sequence length of a computer system call within each detector such that each detector is obscured.

13. (Original) The method as in claim 9, wherein the exchanging the set of detectors includes encoding numerically the detector such that the meaning of the detector is obscured.

14. (Original) The method as in claim 9, wherein the matching rule includes at least one criterion for each field in each detector that is to be matched before a match is validated, and wherein each field includes a sequence of at least one computer system calls.

15. (Currently Amended) A method of providing detection of machine-readable media from an unauthorized usage, the method comprising:

sending by a server a series of behavioral questions for a process residing on a client, wherein the series of behavioral questions comprise a series of different types of system calls and an identifier specifying media associated with the system calls;

receiving at the server a response from the client;

evaluating the response from the process to the series of behavioral questions;

detecting an unauthorized behavior of the process based on the evaluating; and

communicating the detection of the unauthorized behavior of the process among a plurality of other servers, so that the plurality of other servers are enabled to update their series of behavioral questions based in part on the detected unauthorized behavior.

16. (Currently Amended) A server to protect media from unauthorized usage, the system comprising:

a transceiver to send and receive data over the network; and

a program to perform actions when executed that include:

sending a detector to a client, the detector comprising a sequence of different types of system calls, and is associated with a life span that when exceeded inactivates the use of the detector for detecting an unauthorized process;

receiving a response to the detector from the client,

detecting a presence of [[an]]the unauthorized process on the client based on the response and a matching rule associated with the detector, and

updating a database of memory detectors for a previously undetected and unauthorized process on the client such that the database of memory detectors evolves over time.

17. (Original) The system as in claim 16 further including employing the client to access the media.

18. (Original) The system as in claim 16, wherein the sending of the detector includes adjusting the frequency of a class of detectors sent in response to changes in responses from each

client, such that the class of detectors includes at least one of a self-detector, a memory detector, and a novel detector.

19. (Currently Amended) The system as in claim 16, wherein the updating further includes eliminating detectors in the database that exceed [[a]]the predetermined detector life span.

20. (Original) The system as in claim 16, wherein the matching rule includes at least one criterion for a field in the detector to be matched before a match is validated, and wherein the field includes a sequence of at least one computer system calls.

21. (Previously Presented) A system to protect media from unauthorized usage, the system comprising:

a server to send media to a client; and

a program to perform actions when executed that include:

sending a detector to the client;

receiving a response to the detector from the client;

detecting a presence of an unauthorized process on the client based on the response and a matching rule associated with the detector, wherein the detecting includes executing a Rabin-Karp algorithm of prime numbers and a sliding window across the response and the detector; and

updating a database of memory detectors for a previously undetected and unauthorized process on the client such that the database of memory detectors evolves over time.

22. (Currently Amended) A computer readable medium having stored thereon a data structure to provide a detector pattern for use in data integrity of machine-readable media, the data structure comprising:

a plurality of data fields associated with a matching rule to validate a match of the plurality of data fields from a response to the data structure, and wherein at least one data field in the plurality of data fields indicates a media associated with the detector pattern and each of the

remaining data fields in the plurality of data fields comprises [[a]] different types of computer system calls ~~call~~.

23. (Currently Amended) A machine readable medium that provides instructions which, when executed by at least one processor, cause said processor to perform operations comprising:

sending a plurality of different detectors ~~detector~~ to a client process, wherein each detector within the plurality of detectors comprise a different sequence of different types of system calls;

receiving a response to [[the]] each of the plurality of different detectors ~~detector~~ from the client process;

detecting a presence of an unauthorized behavior on the client based upon the response and a matching rule that is associated with the plurality of different detectors ~~detector~~ sent; and

updating a database of memory detectors for a previously unseen and unauthorized behavior of the client process such that the memory database evolves over time, and wherein each memory detector comprises a sequence of different types of system calls that is associated with an unauthorized client process alteration.

24. (Original) The medium as in claim 23, wherein the detector further includes at least one of a self-detector, a memory detector, and a novel detector.

25. (Original) The medium as in claim 23, wherein the detector detects the presence of an unauthorized substantially simultaneously executing client process.

26. (Original) The medium as in claim 23, wherein the sending of the detector further includes varying a sequence length of computer system calls within the detector such that the meaning of the detector is obscured.

27. (Original) The medium as in claim 23, wherein the sending of the detector further includes encoding numerically the detector such that the meaning of the detector is obscured.

28. (New) The method of Claim 1, wherein associated with the detector is a life span defining a length of time that the detector is considered active on the client device, and wherein, when the life span for the detector is exceeded, the detector is inactivated.